(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 May 2002 (02.05.2002)

PCT

(10) International Publication Number
WO 02/35453 A1

(51) International Patent Classification[7]: G06K 9/00

(21) International Application Number: PCT/KR01/01798

(22) International Filing Date: 24 October 2001 (24.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

2000/62538	24 October 2000 (24.10.2000)	KR
2000/30384 U	31 October 2000 (31.10.2000)	KR
2000/30385 U	31 October 2000 (31.10.2000)	KR

(71) Applicant *(for all designated States except US)*: **ALPHA ENGINEERING CO., LTD.** [KR/KR]; 129-414, Yongdu-dong, Dongdaimun-gu, Seoul 130-070 (KR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LEE, Deunggu** [KR/KR]; B-La1, Deokhwa Villa, 32-12, Hwayang-dong, Gwangjin-gu, Seoul 143-916 (KR).

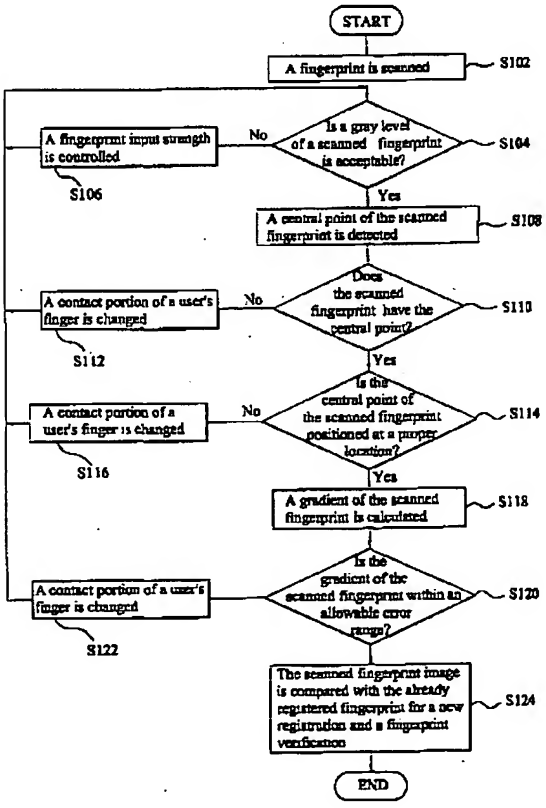
(74) Agents: **JUNG, Sesung** et al.; 6F, Yosam Bldg., 648-23, Yoksam-dong, Gangnam-gu, Seoul 135-748 (KR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,

[Continued on next page]

(54) Title: FINGERPRINT IDENTIFYING METHOD AND SECURITY SYSTEM USING THE SAME



(57) Abstract: A fingerprint identification method includes a) determining a quality of a scanned fingerprint image, b) detecting a central point of the scanned fingerprint image when the quality of the scanned fingerprint image is acceptable, c) calculating a gradient of the scanned fingerprint image when the central point the scanned fingerprint image is located with a designated region, and d) determining whether the gradient of the scanned fingerprint imgae is within an allowable error range.

WO 02/35453 A1

CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

FINGERPRINT IDENTIFYING METHOD AND SECURITY SYSTEM USING THE SAME

Technical Field

The present invention relates to a fingerprint identifying method and a security system using the same.

Background Art

A conventional fingerprint identification system identifies a fingerprint in such a way that a fingerprint of a user is scanned by an image input apparatus such as a scanner, and a scanned fingerprint image is compared with a registered fingerprint data stored in fingerprint database by using ridges and minutiae of a fingerprint.

However, the conventional fingerprint identification system has many difficulties in determining whether the input fingerprint is identical to the registered fingerprint or not. *For example*, when the fingerprint image is very oily or very dry, or when a scanned portion of a fingerprint is too partial to perform a fingerprint identification, it is very difficult to identify or verify the input fingerprint.

In other words, since the conventional fingerprint identification system compares the input fingerprint image with the registered fingerprint image regardless of a quality state of the input fingerprint, when a fingerprint is not properly scanned, it is very difficult to properly identify a fingerprint.

In addition, the convention fingerprint identification system does not let a user know whether the input fingerprint is acceptable or not immediately after the fingerprint is scanned, and why the input fingerprint is unacceptable. The user therefore has to perform all procedure from the beginning for fingerprint identification when the input fingerprint is unacceptable. It is very inconvenient.

Disclosure of Invention

To overcome the problems described above, preferred embodiments of the present invention provide a fingerprint identifying method which can provide a high quality fingerprint image.

It is another object of the present invention to provide a fingerprint identification method, which can provide a convenient fingerprint identification.

It is another object of the present invention to provide a security system with a high security and a convenient fingerprint identification.

In order to achieve the above object, the preferred embodiments of the present invention provide a fingerprint identification method, comprising: a) determining a quality of a scanned fingerprint image; b) detecting a central point of the scanned fingerprint image when the quality of the scanned fingerprint image is acceptable; c) calculating a gradient of the scanned fingerprint image when the central point the scanned fingerprint image is located within a designated region; and d) determining whether the gradient of the scanned fingerprint imgae is within an allowable error range.

The step of (a) includes subdividing the scanned fingerprint into a plurality of blocks; calculating a gray level of each of the plurality of the blocks to determine whether the block is dry or oily; and determing whether the total number of the dry blocks or the total number of the oily blocks is greater than a critical value or not, wherein the fingerprint is discriminated as unacceptable when either the total number of the dry blocks or the total number of the oily blocks is greater than the critical value.

The step of (b) includes designating a boundary region of the central point by calculating a curvature of the scanned fingerprint image; determining whether the central point of the scanned fingerprint image exists or not; detecting the central point of the scanned fingerprint image; and verifying the detected central point of the scanned fingerprint image using a Poincare index.

The step of (c) includes drawing an imaginary line to pass through the central point of the scanned fingerprint; calculating direction angles of normal lines at crossing points of the imaginary line and ridges of the fingerprint; comparing the direction angles of the normal lines of the right ridges of the central point of the scanned fingerprint with the direction angles of the normal lines of the left ridges of the central point of the scanned fingerprint; and changing a direction of the imaginary line until an offset value of the direction angles of the normal lines of the right ridges and the left ridges becomes approximate to "0", wherein a direction of a perpendicular line to the finally set imaginary line is decided as a gradient of the scanned fingerprint when the offset value becomes approximate to "0".

The present invention further provides an entrance door system, comprising: a fingerprint scanning portion scanning a fingerprint; a memory portion storing a registered fingerprint; a controller a) determining a quality of the scanned fingerprint image, b) detecting a central point of the scanned fingerprint image when the quality of the scanned fingerprint image is acceptable, c) calculating a gradient of the scanned fingerprint image when the central point of the scanned fingerprint image is located within a designated region, d) determining whether the gradient of the scanned fingerprint imgae is within an

allowable error range, and e) determining whether the scanned fingerprint is identical to the registered fingerprint or not when the gradient of the scanned fingerprint imgae is within the allowable error range; and an entrance door actuator opening or closing an entrance door in response to a control signal output from the controller.

The entrance door system further includes a display panel displaying a text message stored in the memory portion; a voice output portion outputing a voice message stored in the memory portion; a key pad portion including digit keys, letter keys and function keys; and a call portion for calling an inside staff member.

The present invention further provides a cash dispenser, comprising: a bank card reader determining whether a fingerprint written on the bank card inserted thereinto is identical to a registered fingerprint or not; a fingerprint scanning portion scanning a fingerprint; a memory portion storing the registered fingerprint; and a controller a) determining a quality of the scanned fingerprint image, b) detecting a central point of the scanned fingerprint image when the quality of the scanned fingerprint image is acceptable, c) calculating a gradient of the scanned fingerprint image when the central point the scanned fingerprint image is located within a designated region, d) determining whether the gradient of the scanned fingerprint imgae is within an allowable error range, and e) determining whether the scanned fingerprint is identical to the registered fingerprint or not when the gradient of the scanned fingerprint imgae is within the allowable error range, wherein the cash dispenser operates in response to a control signal output from the controller.

The cash dispenser further includes a display panel displaying a text message stored in the memory portion; a voice output portion outputing a voice message stored in the memory portion; a key pad portion including digit keys, letter keys and function keys; and a call portion for calling a bank clerk.

The fingerprint identification method according to the present invention can provide a high quality fingerprint identification. Also, since a user can know whether the input fingerprint is acceptable or not immediately after the fingerprint is scanned, and if not, why the input fingerprint is unacceptable, it is very convenient. In addition, due to a high quality fingerprint identification, the system such as the entrance door system and the cash dispenser can have a high security.

Brief Description of Drawings

For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the

accompanying drawings, in which like reference numerals denote like parts, and in which:

FIG. 1 is a flow chart illustrating a fingerprint identification method according to an embodiment of the present invention;

FIGs. 2A to 2C are photographs illustrating a process for calculating a quality of a scanned fingerprint image;

FIGs. 3A and 3B are photographs illustrating fingerprint images having unacceptable quality;

FIGs. 4A to 4C are photographs illustrating a process of detecting a central point of a scanned fingerprint image;

FIG. 5 shows a process of calculating a gradient of a scanned fingerprint image;

FIGs. 6A and 6B are photographs illustrating a gradient of a scanned fingerprint image;

FIG. 7 is a block diagram illustrating an entrance door system in which the fingerprint identification method of FIG. 1 is employed;

FIG. 8 shows a front panel of the entrance door system of FIG. 7;

FIG. 9 is a flow chart illustrating operation of the entrance door system of FIG. 7;

FIG. 10 is a block diagram illustrating a cash dispenser in which the fingerprint identification method of FIG. 1 is employed; and

FIG. 11 is a block diagram an appearance of the cash dispenser of FIG. 10.

Best Mode for Carrying Out the Invention

Reference will now be made in detail to preferred embodiments of the present invention, example of which is illustrated in the accompanying drawings.

FIG. 1 is a flow chart illustrating a fingerprint identification method according to an embodiment of the present invention. FIGs. 2A to 2C are photographs illustrating a process for calculating a quality of a scanned fingerprint image. FIGs. 3A and 3B are photographs illustrating fingerprint images having unacceptable quality. FIGs. 4A to 4C are photographs illustrating a process of detecting a central point of a scanned fingerprint image. FIG. 5 shows a process of calculating a gradient of a scanned fingerprint image. FIGs. 6A and 6B are photographs illustrating a gradient of a scanned fingerprint image.

The fingerprint identification method according to the present invention is described below with reference to FIG. 1 to FIG. 6B

First, a user rests his/her finger (e.g., thumb) on a fingerprint input means such as a fingerprint scanner to scan his/her fingerprint (step S102).

A quality of the scanned fingerprint image is decided (step S104). In order to

decide a quality of the scanned fingerprint image, as shown in FIGs. 2A to 2C, the scanned fingerprint image is subdivided into a plurality of blocks. A gray level of each of a plurality of the blocks is calculated. When the gray level of a certain block is relatively low, the block is discriminated as an oily block. When the gray level of the block is relatively high, the block is discriminated as a dry block. Thereafter, the total number of the oily blocks and the dry blocks are calculated, respectively. When the total number of the oily blocks is greater than a critical value, as shown in FIG. 3A, the scanned fingerprint image is discriminated as an oily fingerprint image which is unacceptable. Also, when the total number of the dry blocks is greater than a critical value, as shown in FIG. 3B, the scanned fingerprint image is discriminated as a dry fingerprint image which is unacceptable.

Subsequently, when the scanned fingerprint image is discriminated as unacceptable, a fingerprint input strength is controlled (step S106). When the scanned fingerprint image is discriminated as an oily fingerprint image, a text message or a voice message that asks to rest his finger on the fingerprint input more slightly than before is output to a user through a display panel or a voice output means such as a speaker. Also, when the scanned fingerprint image is discriminated as a dry fingerprint image, a text message or a voice message that asks to rest his finger on the fingerprint input more strongly than before is output to a user through a display panel or a voice output means such as a speaker.

When a quality of the scanned fingerprint image is discriminated as acceptable by repeatedly performing the step S106, a central point of the scanned fingerprint is detected (step S108). In order to detect a central point of the scanned fingerprint, a boundary region is first designated by calculating a curvature of the scanned fingerprint image as shown in FIG. 4A, and a central point of the scanned fingerprint is detected. The detected central point of the scanned fingerprint image is verified using a Poincare index (step S110). In FIGs. 4B and 4C, dots "•" denote a central point of the fingerprint image.

When a central point of the scanned fingerprint is not detected, a text message or a voice message that asks to change a contact portion of a user's finger is output to a user through a display panel or a voice output means such as a speaker (step S112).

When a central point of the scanned fingerprint is detected, it is determined whether a central point of the scanned fingerprint is positioned at a proper location or not (step S114). When a central point of the scanned fingerprint is not positioned within a designated region as shown in FIG. 4C, a text message or a voice message that asks to change a contact portion of a user's fingerprint is output to a user through a display panel or a voice output means such as a speaker (step S116).

When a central point of the scanned fingerprint is positioned within a designated region as shown in FIG. 4B, a gradient of the scanned fingerprint is calculated (step S118). In order to calculate a gradient of the scanned fingerprint, as shown in FIG. 5, an imaginary line is first drawn to pass through a central point of the scanned fingerprint. Direction angles of normal lines at crossing points of the imaginary line and the ridges of the fingerprint are calculated. The direction angles of the normal lines of the right ridges of a central point of the scanned fingerprint are compared with the direction angles of the normal lines of the left ridges of a central point of the scanned fingerprint. Until an offset value of the direction angles of the normal lines of the right ridges and the left ridges becomes approximate to "0", a direction of the imaginary line is changed. When the offset value becomes approximate to "0", a direction of a perpendicular line to the finally set imaginary line is decided as a gradient of the scanned fingerprint. In FIGs. 6A and 6B, arrows denote a gradient of the scanned fingerprint.

Thereafter, it is determined whether the gradient of the scanned fingerprint is within an allowable error range or not (step S120). When the gradient of the scanned fingerprint is not within an allowable error range, a text message or a voice message that asks to change a gradient of a fingerprint is output to a user through a display panel or a voice output means such as a speaker (step S122). When the gradient of the scanned fingerprint is within an allowable error range, the scanned fingerprint image is compared with the already registered fingerprint for a new registration and a fingerprint verification (step S124).

The fingerprint identification method according to the present invention can be used in various industrial fields.

FIG. 7 is a block diagram illustrating an entrance door system in which the fingerprint identification method of FIG. 1 is employed. FIG. 8 shows a front panel of the entrance door system of FIG. 7.

The entrance door system according to the present invention includes a sensor portion 12, a keypad portion 14, a call portion 16, a voice output portion 18, a fingerprint input portion 22, a digital processing portion 24, a memory portion 26, a buffer portion 28, a fingerprint input portion shutter 32, a controller 34, a comparator 36, a video camera 3, a video phone 42, an entrance door actuator 44, a display panel 48, and a lamp 52.

The sensor portion 12 detects a person when the person is positioned within a predetermined distance from an entrance door. The keypad portion 14 includes a plurality of key buttons such as digit keys, letter keys and function keys. The call portion 16 is used to call a person in, *e.g.*, a security area. The voice output portion 18 outputs a voice

message to a person outside, *e.g.*, a security area. The fingerprint input portion 22 scans and receives a fingerprint image. The digital processing portion 24 reads the scanned fingerprint image. The memory portion 26 stores text messages, voice messages, registered fingerprint images, passwords, identification (ID) numbers, user formations, other information required to perform a fingerprint identification (*e.g.*, a standard gray level and allowable error range of a gradient of the fingerprint image), etc. The buffer portion 28 temporarily stores data input through the key pad portion 14 or a fingerprint image read by the digital processing portion 24. The fingerprint input portion shutter 32 opens or close a cover of the fingerprint input portion 22. The controller 34 controls all components of the entrance door system, and determines whether the scanned fingerprint image is acceptable or not to output a control signal. The comparator 36 compares an input password, an input ID number and an input fingerprint with registered ones under a control of the controller 34, respectively. The video phone 42 displays an image of a person outside, *e.g.*, a security area, and a person in *e.g.*, a security area manipulates the video phone 42 to generate a control signal that opens an entrance door. The entrance door actuator 44 closes or opens the entrance door in response to a control signal from the controller 34. The display panel 48 displays a text message or digits input through the key pad portion 14. The lamp 52 indicates an operation state of the sensor portion 12 and the entrance door system.

When a person stands in front of the entrance door within a predetermined distance from the entrance door system of FIG. 7, the sensor portion 12 detects the person to output a detecting signal to the controller 34. The controller 34 receives the detecting signal to output a text message or a voice message stored in the memory portion 26 through the display panel 48 or the voice output portion 18 as follows: "Welcome. If you are a guest, please push the call button".

If a detected person is a guest, when the guest pushes the call button of the call portion 16, a staff member inside the entrance door monitors an image of the guest taken by the video camera 38 arranged on the entrance door through the video phone 42. When the staff member outputs a door open signal, the controller 34 receives the door open signal to output a control signal to the entrance door actuator 44, thereby opening the entrance door. After a predetermined time period, the controller 34 outputs a control signal to the entrance door actuator 44 to close the entrance door

Meanwhile, when the person standing in front of the entrance door is a staff member, the person first has to input a password through the key pad portion 14. The input password is temporarily stored in the buffer portion 28 and transferred to the controller 34 and the comparator 36. The controller 34 determines whether the input password is

identical to the registered password or not using the comparator 36. When the input password is identical to the registered password, the controller 34 outputs a control signal to the fingerprint input portion shutter 32 to open a cover of the fingerprint input portion 22. When the cover of the fingerprint input portion 22 is opened, the controller 34 outputs a text message or a voice message through the display panel 48 or the voice output portion 18 as follows: "Please input your fingerprint".

The scanned fingerprint image is read by the digital processing portion 24 and the read fingerprint image is temporarily stored in the buffer portion 28. At the same time, the controller 34 calculates a quality of the read fingerprint image to determine whether the scanned fingerprint image is acceptable or not by the method described in the step S104 of FIG. 1. When the scanned fingerprint image is discriminated as unacceptable, a fingerprint input strength is controlled. That is, when the scanned fingerprint image is discriminated as an oily fingerprint image which is unacceptable, the controller 34 outputs a text message or a voice message that asks to rest his finger on the fingerprint input more slightly than before through the display panel 48 or the voice output portion 18 as follows: "The fingerprint is too oily. Please try again". Also, when the scanned fingerprint image is discriminated as a dry fingerprint image, the controller 34 outputs a text message or a voice message that asks to rest his finger on the fingerprint input more strongly than before through the display panel 48 or the voice output portion 18 as follows: "The fingerprint is too dry. Please try again".

When the scanned fingerprint image is discriminated as acceptable by repeatedly performing the step S106, a central point of the scanned fingerprint is detected. When a central point does not exists in the scanned fingerprint, or when a central point of the scanned fingerprint is detected but is not positioned within a designated region, the controller outputs a text message or a voice message as follows: "Please change a contact portion of your finger and try again".

When a central point of the scanned fingerprint is positioned within a designated region, a gradient of the scanned fingerprint is calculated in the method described in the step S118. The controller 34 determines whether the gradient of the scanned fingerprint is within an allowable error range. When the gradient of the scanned fingerprint is not within an allowable error range, the controller 34 outputs a text message or a voice message that asks to change a gradient of a fingerprint. When the gradient of the scanned fingerprint is within allowable error range, the comparator 36 compares the scanned fingerprint image with the already registered fingerprint. When the scanned fingerprint image is identical to the registered fingerprint, the controller 34 outputs a control signal to the entrance door

actuator 44 in response to an output signal of the comparator 36 to open the entrance door.

The entrance door system of FIG. 7 can be used in, *for example*, a household, a company, or a research institute, which require a high security.

FIG. 9 is a flow chart illustrating operation of the entrance door system of FIG. 7.

When a person stands in front of the entrance door within a predetermined distance from the entrance door system of FIG. 7, the sensor portion 12 detects the person to output a detecting signal to the controller 34 (step S302). The controller 34 receives the detecting signal to output a text message or a voice message stored in the memory portion 26 through the display panel 48 or the voice output portion 18 as follows: "Welcome. If you are a guest, please push the call button" (step S304).

When the guest pushes the call button of the call portion 16, the controller 34 output a text message or a voice message as follows: "Please wait" (step S308). Thereafter, the entrance door system finishes its operation and is initialized.

When the person does not push the call button in a predetermined time period, the controller 34 outputs a text message or a voice message as follows: "Please input your password and push a confirm button" (step S310).

When a password is input through the key pad portion 14, the controller 34 determines whether the input password is identical to the registered password or not (step S312). When the input password is not identical to the registered password, the controller 34 outputs a text message or a voice message as follows: "Password is not correct. Would you please push the call button? (step S314).

The controller 34 determines whether the call button is pushed or not (step S316). When the call button is pushed, the entrance door system outputs a text message or a voice message of the step S308 and finishes its operation. When the call button is not pushed in a predetermined time period, the controller 34 outputs a text message or a voice message as follows: "Please input your password and push the confirm button".

When the input password is identical to the registered password, the controller 34 outputs a text message or a voice message as follows: "Please input your fingerprint" (step S318). Thereafter, the controller 34 outputs a control signal to the fingerprint input portion shutter 32 to open a cover of the fingerprint input portion 22 (step 320).

The controller 34 calculates a quality of the scanned fingerprint image to determine whether the scanned fingerprint image is acceptable or not by the method described in the step S104 of FIG. 1 (step S322). When the scanned fingerprint image is discriminated as unacceptable, a fingerprint input strength is controlled. That is, when the scanned fingerprint image is discriminated as an oily fingerprint image which is

unacceptable, the controller 34 outputs a text message or a voice message that asks to rest his finger on the fingerprint input more slightly than before through the display panel 48 or the voice output portion 18 as follows: "The fingerprint is too oily. Please try again". Also, when the scanned fingerprint image is discriminated as a dry fingerprint image, the controller 34 outputs a text message or a voice message that asks to rest his finger on the fingerprint input more strongly than before through the display panel 48 or the voice output portion 18 as follows: "The fingerprint is too dry. Please try again" (step S324).

When a quality of the scanned fingerprint image is discriminated as acceptable, a central point of the scanned fingerprint is detected (step S326). When a central point does not exists in the scanned fingerprint, or when a central point of the scanned fingerprint is detected but is not positioned within a designated region, the controller outputs a text message or a voice message as follows: "Please change a contact portion of your finger and try again" (step S328).

When a central point of the scanned fingerprint is positioned within a designated region, a gradient of the scanned fingerprint is calculated in the method described in the step S118 of FIG. 1. The controller 34 determines whether the gradient of the scanned fingerprint is within an allowable error range (step S330). When the gradient of the scanned fingerprint is not within allowable error range, the controller 34 outputs a text message or a voice message as follows: "Change a gradient of a fingerprint" (step S332).

When the gradient of the scanned fingerprint is within allowable error range, the controller 34 compares the scanned fingerprint image with the already registered fingerprint. When the scanned fingerprint image is identical to the registered fingerprint, the controller 34 outputs a text message or a voice message as follows: "Thank you. The fingerprint is identified". At the same time, the controller 34 outputs a control signal to the fingerprint input portion shutter 32 to close the cover of the fingerprint input portion 22 (step S336).

Thereafter, the controller 34 outputs a control signal to the entrance door actuator 44 to open the entrance door (step S338). After the predetermined time period is passed (step S340), the controller 34 outputs a control signal to the entrance door actuator 44 to close the entrance door (step S342).

FIG. 10 is a block diagram illustrating a cash dispenser according to the present invention. FIG. 11 is a block diagram an appearance of the cash dispenser of FIG. 10.

The cash dispenser according to the present invention includes a sensor portion 212, a bank card reader 214, a call portion 216, a voice output portion 218, a fingerprint input portion 222, a digital processing portion 224, a memory portion 226, an image

memory portion 227, a buffer portion 228, a fingerprint input portion shutter 232, a controller 234, a comparator 236, a driver 238, a call connection module 242, a camera 244, a display panel 246, a cash outlet 248, and a receipt outlet 250. At this point, the memory portion 226 stores voice messages, and the image memory portion 227 stores fingerprint images.

When the sensor portion 212 detects a person standing in front of the cash dispenser, a text message or a voice message which asks to insert the bank card is output. When the bank card is inserted into the bank card reader 214, the bank card reader 214 reads a fingerprint data written on a magnetic portion of a bank card and stores the fingerprint data in the buffer portion 228 temporarily. At the same time, the fingerprint data is transferred to the controller 234 and the comparator 236. The comparator 236 determines whether the fingerprint data written on the magnetic portion is identical to the registered fingerprint data stored in the image memory portion 227. When the fingerprint data of the bank card is identical to the registered fingerprint data, the controller 234 outputs a control signal to the fingerprint input portion shutter 232 in response an output signal of the comparator 236 to open a cover of the fingerprint input portion 222. At the same time, the controller 234 outputs a text message or a voice message that asks to input a fingerprint through the display panel 220 or the voice output portion 218.

A user rests his/her finger (*e.g.*, thumb) on the fingerprint input portion 222, and the digital processing portion 224 reads a fingerprint image of the user. The scanned fingerprint image is temporarily stored in the buffer portion 228 and transferred to the controller 234.

At the same time, the controller 234 calculates a quality of the read fingerprint image to determine whether the scanned fingerprint image is acceptable or not by the method described in the step S104 of FIG. 1. When the scanned fingerprint image is discriminated as unacceptable, a fingerprint input strength is controlled. That is, when the scanned fingerprint image is discriminated as an oily fingerprint image which is unacceptable, the controller 234 outputs a text message or a voice message that asks to rest his finger on the fingerprint input more slightly than before through the display panel 246 or the voice output portion 218 as follows: "The fingerprint is too oily. Please try again". Also, when the scanned fingerprint image is discriminated as a dry fingerprint image, the controller 234 outputs a text message or a voice message that asks to rest his finger on the fingerprint input more strongly than before through the display panel 48 or the voice output portion 218 as follows: "The fingerprint is too dry. Please try again".

When the scanned fingerprint image is discriminated as acceptable, a central point

of the scanned fingerprint is detected by the method described in the step S110 of FIG. 1. When a central point does not exists in the scanned fingerprint, or when a central point of the scanned fingerprint is detected but is not positioned within a designated region, the controller outputs a text message or a voice message as follows: "Please change a contact portion of your finger and try again".

When a central point of the scanned fingerprint is positioned within a designated region, a gradient of the scanned fingerprint is calculated in the method described in the step S118 of FIG. 1. The controller 234 determines whether the gradient of the scanned fingerprint is within allowable error range. When the gradient of the scanned fingerprint is not within allowable error range, the controller 234 outputs a text message or a voice message that asks to change a gradient of a fingerprint. When the gradient of the scanned fingerprint is within allowable error range, the controller 234 compares the scanned fingerprint image with the already registered fingerprint. When the scanned fingerprint image is identical to the registered fingerprint, the controller 234 outputs a control signal to allow a user to receive a service of the cash dispenser.

Meanwhile, when a user pushes a call button of the call portion 216 due to, *for example*, abnormal operation of the cash dispenser, the driver 238 provides a communication between the call portion 216 and the call connection module 242, thereby calling a bank clerk.

Industrial Applicability

As described herein before, the fingerprint identification method according to the present invention can provide a high quality fingerprint identification. Also, since a user can know whether the input fingerprint is acceptable or not immediately after the fingerprint is scanned, it is very convenient. In addition, due to a high quality fingerprint identification, the system such as the entrance door system and the cash dispenser can have a high security.

While the invention has been particularly shown and described with reference to preferred embodiments thereof, it will be understood by those skilled in the art that the foregoing and other changes in form and details may be made therein without departing from the spirit and scope of the invention.

What is claimed is:

1. A fingerprint identification method, comprising:

a) determining a quality of a scanned fingerprint image;

b) detecting a central point of the scanned fingerprint image when the quality of the scanned fingerprint image is acceptable;

c) calculating a gradient of the scanned fingerprint image when the central point the scanned fingerprint image is located with a designated region; and

d) determining whether the gradient of the scanned fingerprint imgae is within an allowable error range.

2. The method of claim 1, wherein the step of (a) includes

subdividing the scanned fingerprint into a plurality of blocks;

calculating a gray level of each of the plurality of the blocks to determine whether the block is dry or oily; and

determining whether the total number of the dry blocks or the total number of the oily blocks is greater than a critical value or not,

wherein the fingerprint is discriminated as unacceptabl when either the total number of the dry blocks or the total number of the oily blocks is greater than the critical value.

3. The method of claim 1, wherien the step of (b) includes

designating a boundary region of the central point by calculating a curvature of the scanned fingerprint image

determining whether the central point of the scanned fingerprint image exists or not;

detecting the central point of the scanned fingerprint image; and

verifying the detected central point of the scanned fingerprint image using a Poincare index.

4. The method of claim 1, wherein the step of (c) includes

drawing an imaginary line to pass through the central point of the scanned fingerprint;

calculating direction angles of normal lines at crossing points of the imaginary line and ridges of the fingerprint;

comparing the direction angles of the normal lines of the right ridges of the central point of the scanned fingerprint with the direction angles of the normal lines of the left ridges of the central point of the scanned fingerprint; and

changing a direction of the imaginary line until an offset value of the direction angles of the normal lines of the right ridges and the left ridges becomes approximate to "0",

wherein a direction of a perpendicular line to the finally set imaginary line is decided as a gradient of the scanned fingerprint when the offset value becomes approximate to "0".

5. An entrance door system, comprising:

a fingerprint scanning portion scanning a fingerprint;

a memory portion storing a registered fingerprint;

a controller a) determining a quality of the scanned fingerprint image, b) detecting a central point of the scanned fingerprint image when the quality of the scanned fingerprint image is acceptable, c) calculating a gradient of the scanned fingerprint image when the central point the scanned fingerprint image is located with a designated region, d) determining whether the gradient of the scanned fingerprint imgae is within an allowable error range, and e) determining whether the scanned fingerprint is identical to the registered fingerprint or not when the gradient of the scanned fingerprint imgae is within the allowable error range; and

an entrance door actuator opening or closing an entrance door in response to a control signal output from the controller.

6. The system of claim 5, wherein the step of (a) includes

subdividing the scanned fingerprint into a plurality of blocks;

calculating a gray level of each of the plurality of the blocks to determine whether the block is dry or oily; and

determing whether the total number of the dry blocks or the total number of the oily blocks is greater than a critical value or not,

wherein the fingerprint is discriminated as unacceptabl when either the total number of the dry blocks or the total number of the oily blocks is greater than the critical value.

7. The system of claim 5, wherien the step of (b) includes

designating a boundary region of the central point by calculating a curvature of the scanned fingerprint image

determining whether the central point of the scanned fingerprint image exists or not;

detecting the detecting the central point of the scanned fingerprint image; and

verifying the detected central point of the scanned fingerprint image using a Poincare index.

8. The system of claim 5, wherein the step of (c) includes

drawing an imaginary line to pass through the central point of the scanned fingerprint;

calculating direction angles of normal lines at crossing points of the imaginary line and ridges of the fingerprint;

comparing the direction angles of the normal lines of the right ridges of the central point of the scanned fingerprint with the direction angles of the normal lines of the left ridges of the central point of the scanned fingerprint; and

changing a direction of the imaginary line until an offset value of the direction angles of the normal lines of the right ridges and the left ridges becomes approximate to "0",

wherein a direction of a perpendicular line to the finally set imaginary line is decided as a gradient of the scanned fingerprint when the offset value becomes approximate to "0".

9. The system of claim 5, further comprising,

a display panel displaying a text message stored in the memory portion;

a voice output portion outputing a voice message stored in the memory portion;

a key pad portion including digit keys, letter keys and function keys; and

a call portion for calling an inside staff member.

10. A cash dispenser, comprising:

a bank card reader determining whether a fingerprint written on the bank card inserted thereinto is identical to a registered fingerprint or not;

a fingerprint scanning portion scanning a fingerprint;

a memory portion storing the registered fingerprint; and

a controller a) determining a gray level of the scanned fingerprint image, b) detecting a central point of the scanned fingerprint image when the quality of the scanned fingerprint image is acceptable, c) calculating a gradient of the scanned fingerprint image when the central point the scanned fingerprint image is located with a designated region, d) determining whether the gradient of the scanned fingerprint imgae is within an allowable error range, and e) determining whether the scanned fingerprint is identical to the registered fingerprint or not when the gradient of the scanned fingerprint image is within the allowable error range,

wherein the cash dispenser operates in response to a control signal output from the controller.

11. The system of claim 10, wherein the step of (a) includes

subdividing the scanned fingerprint into a plurality of blocks;

calculating a gray level of each of the plurality of the blocks to determine whether the block is dry or oily; and

determining whether the total number of the dry blocks or the total number of the oily blocks is greater than a critical value or not,

wherein the fingerprint is discriminated as unacceptabl when either the total number of the dry blocks or the total number of the oily blocks is greater than the critical value.

12. The system of claim 10, wherien the step of (b) includes

designating a boundary region of the central point by calculating a curvature of the scanned fingerprint image

determining whether the central point of the scanned fingerprint image exists or not;

detecting the detecting the central point of the scanned fingerprint image; and

verifying the detected central point of the scanned fingerprint image using a Poincare index.

13. The system of claim 10, wherein the step of (c) includes

drawing an imaginary line to pass through the central point of the scanned fingerprint;

calculating direction angles of normal lines at crossing points of the imaginary line and ridges of the fingerprint;

comparing the direction angles of the normal lines of the right ridges of the central point of the scanned fingerprint with the direction angles of the normal lines of the left ridges of the central point of the scanned fingerprint; and

changing a direction of the imaginary line until an offset value of the direction angles of the normal lines of the right ridges and the left ridges becomes approximate to "0",

wherein a direction of a perpendicular line to the finally set imaginary line is decided as a gradient of the scanned fingerprint when the offset value becomes approximate to "0".

14. The system of claim 10, further comprising,

a display panel displaying a text message stored in the memory portion;

a voice output portion outputing a voice message stored in the memory portion;

a key pad portion including digit keys, letter keys and function keys; and

a call portion for calling a bank clerk.

FIG. 1

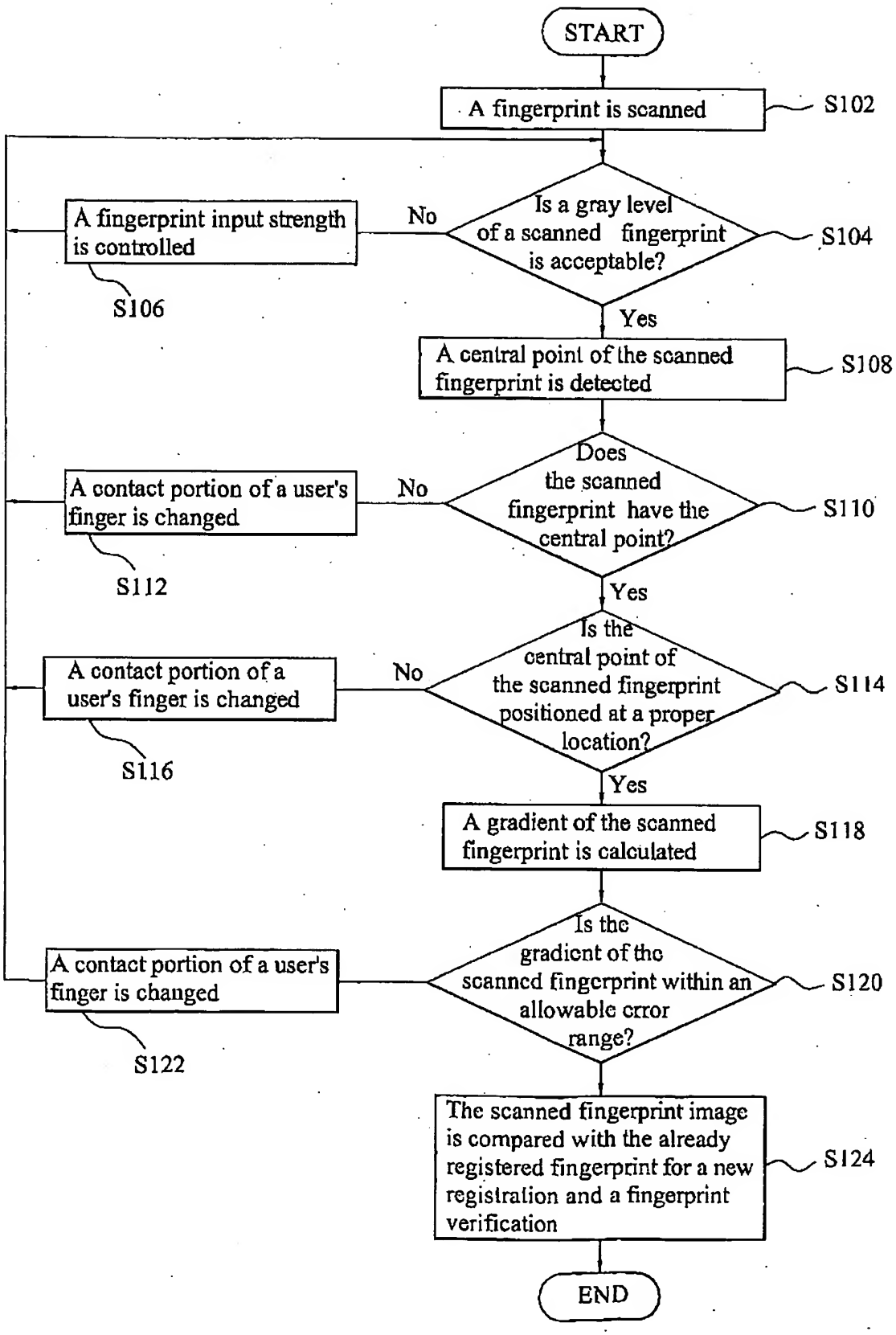

START
A fingerprint is scanned
S102
Is a gray level of a scanned fingerprint is acceptable?
S104
No
A fingerprint input strength is controlled
S106
Yes
A central point of the scanned fingerprint is detected
S108
Does the scanned fingerprint have the central point?
S110
No
A contact portion of a user's finger is changed
S112
Yes
Is the central point of the scanned fingerprint positioned at a proper location?
S114
No
A contact portion of a user's finger is changed
S116
Yes
A gradient of the scanned fingerprint is calculated
S118
Is the gradient of the scanned fingerprint within an allowable error range?
S120
A contact portion of a user's finger is changed
S122
The scanned fingerprint image is compared with the already registered fingerprint for a new registration and a fingerprint verification
S124
END

FIG. 2A

FIG. 2B

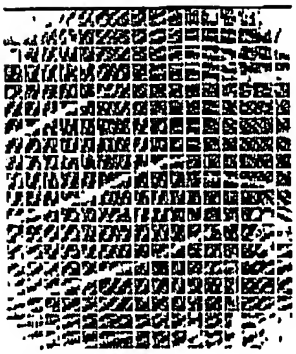


FIG. 2C

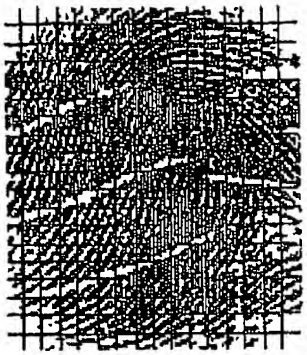


FIG. 3A

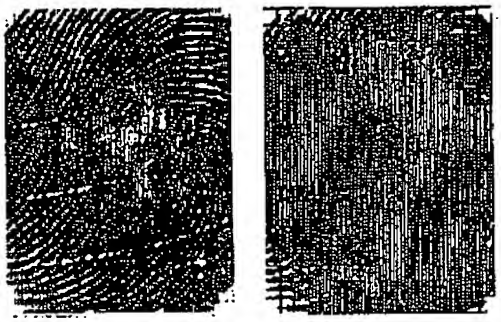
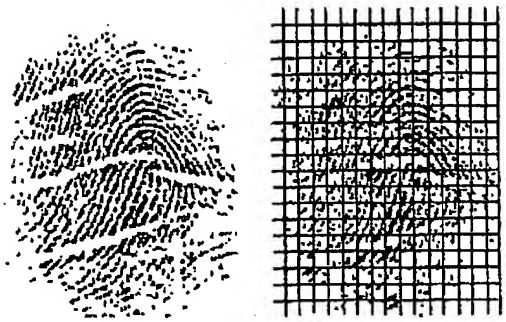


FIG. 3B



BEST AVAILABLE COPY

FIG. 4A

FIG. 4B

FIG. 4C

FIG. 5

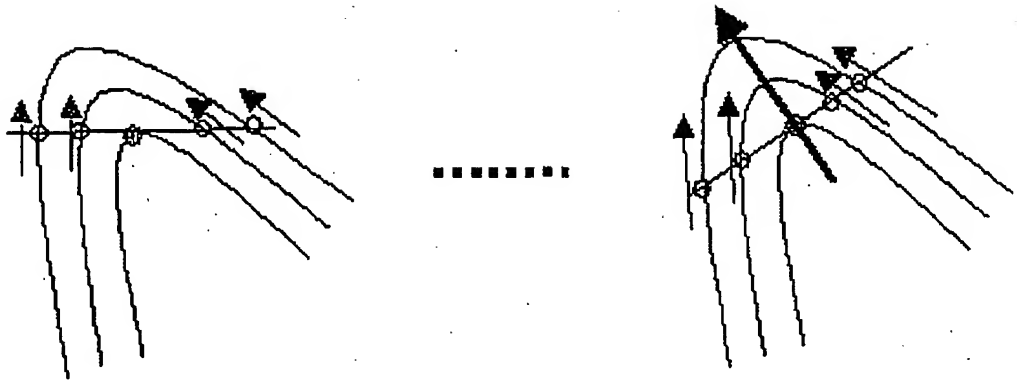


FIG. 6A

FIG. 6B

FIG. 7

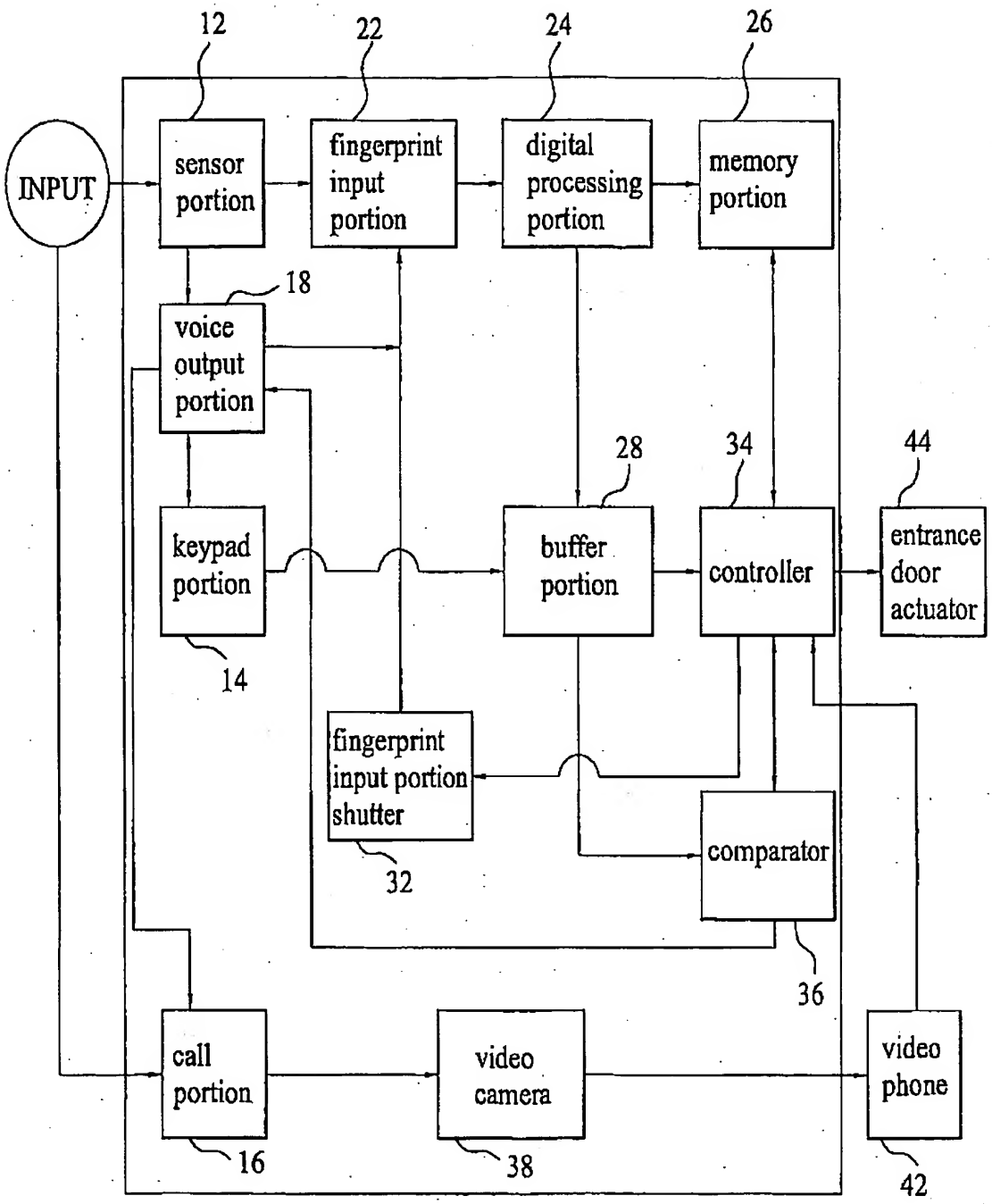

12
22
24
26
INPUT
sensor portion
fingerprint input portion
digital processing portion
memory portion
18
voice output portion
28
34
44
keypad portion
buffer portion
controller
entrance door actuator
14
fingerprint input portion shutter
comparator
32
36
call portion
video camera
video phone
16
38
42

FIG. 8

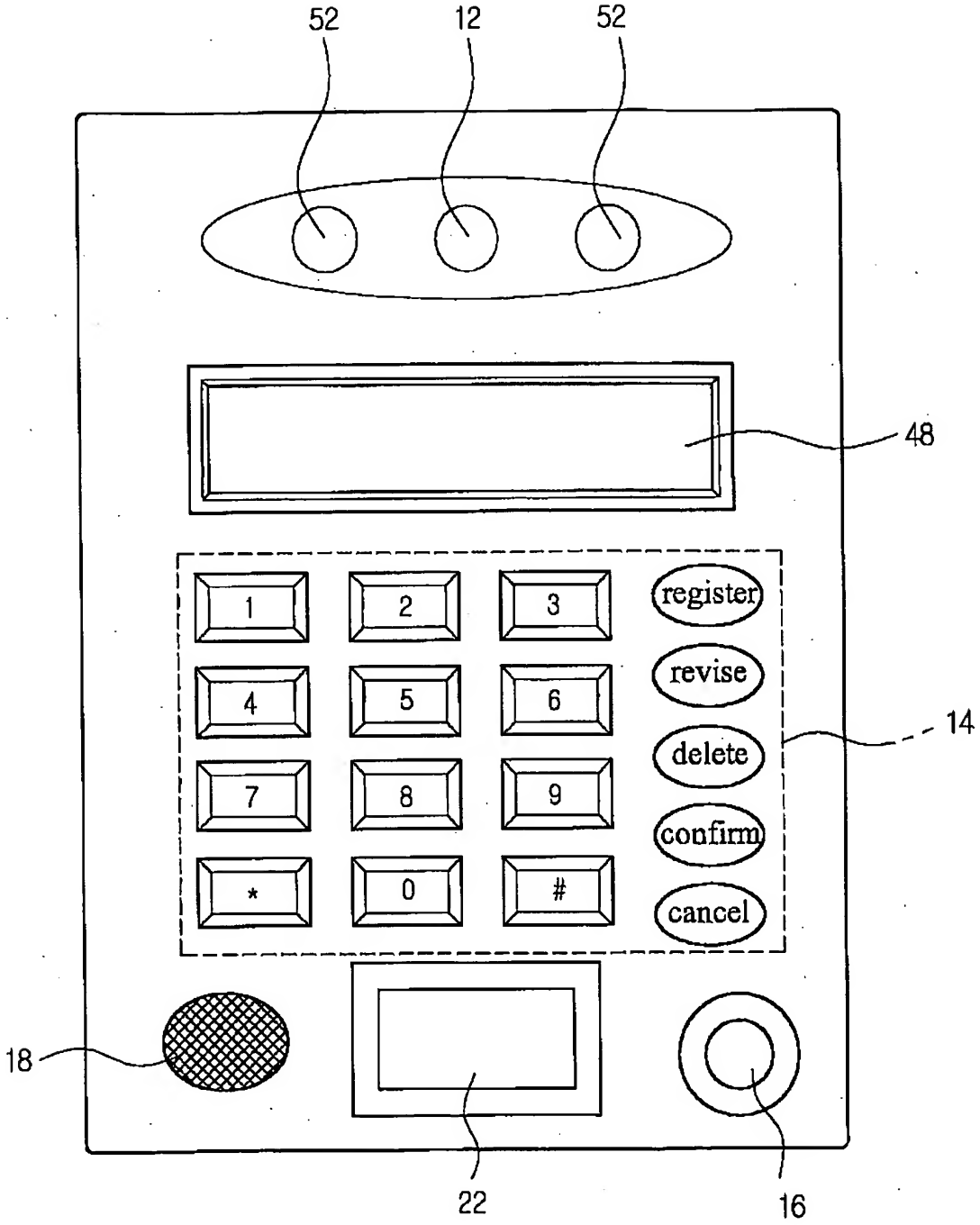

52
12
52
48
1
2
3
register
4
5
6
revise
14
7
8
9
delete
confirm
*
0
#
cancel
18
22
16

FIG. 9

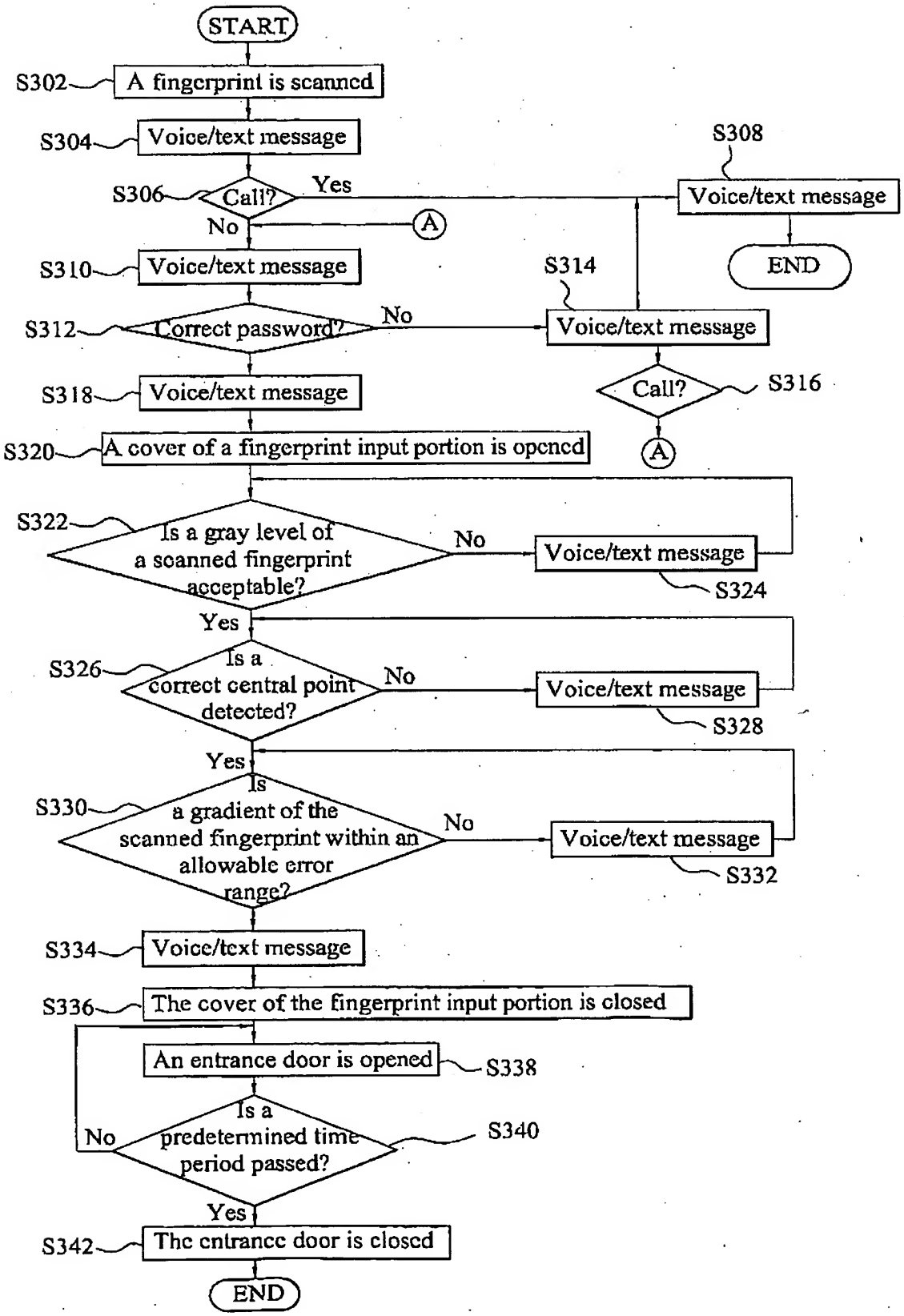

START
S302
A fingerprint is scanned
S304
Voice/text message
S306
Call?
Yes
No
A
S308
Voice/text message
END
S310
Voice/text message
S312
Correct password?
No
S314
Voice/text message
Call?
S316
A
S318
Voice/text message
S320
A cover of a fingerprint input portion is opened
S322
Is a gray level of a scanned fingerprint acceptable?
No
Voice/text message
S324
Yes
S326
Is a correct central point detected?
No
Voice/text message
S328
Yes
S330
Is a gradient of the scanned fingerprint within an allowable error range?
No
Voice/text message
S332
S334
Voice/text message
S336
The cover of the fingerprint input portion is closed
An entrance door is opened
S338
No
Is a predetermined time period passed?
S340
Yes
S342
The entrance door is closed
END

FIG. 10

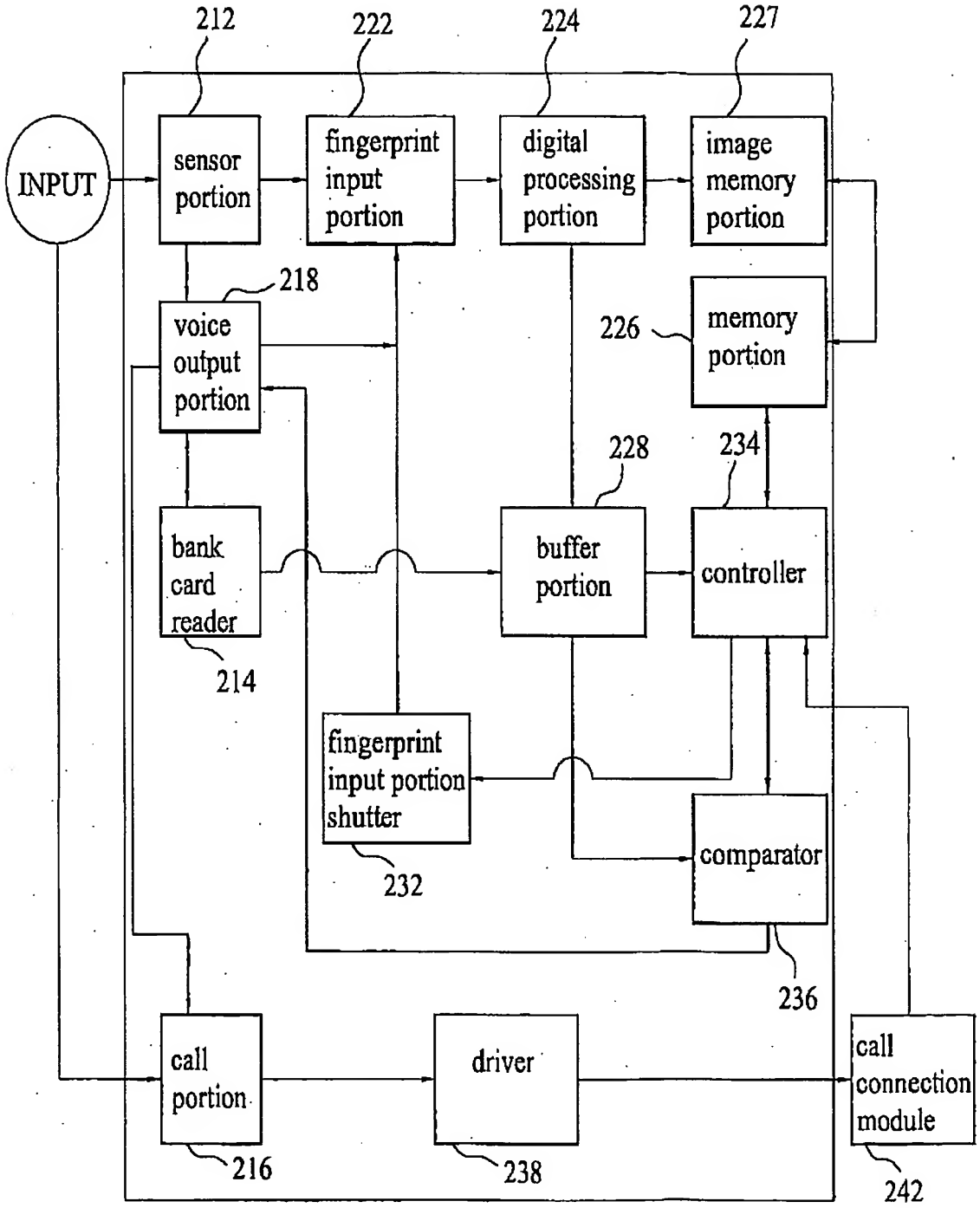
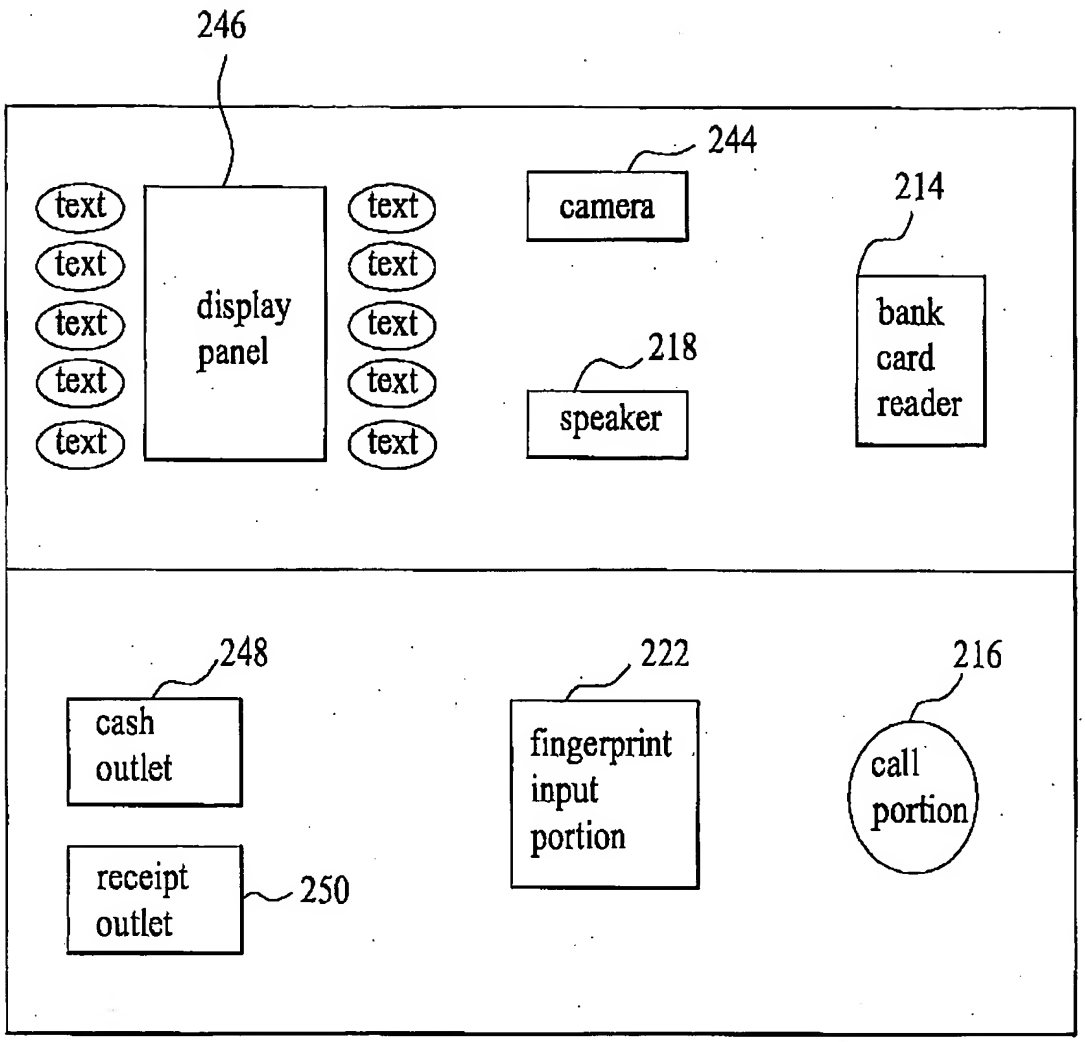

212
222
224
227
INPUT
sensor portion
fingerprint input portion
digital processing portion
image memory portion
218
voice output portion
226
memory portion
228
234
bank card reader
214
buffer portion
controller
fingerprint input portion shutter
232
comparator
236
call portion
216
driver
238
call connection module
242

FIG. 11


246
text
text
text
text
text
display panel
text
text
text
text
text
244
camera
214
bank card reader
218
speaker
248
cash outlet
receipt outlet
250
222
fingerprint input portion
216
call portion

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR01/01798

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 G06K 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC7 G06K, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Patents and patent Applications for invention since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
KIPONET.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US5963656A1(International Business Machines Corporation) 5.OCT.1999 See the abstract and figures	1-14
A	US5796857A1(NEC Corporation) 18.AUG.1998 See the abstract and figures	1-14
A	KR10-1999-74775(PANTECH) 5.OCT.1999 See the abstract AND figures	1-14
A	KR10-1999-73820(PARK KI OK) 5.OCT.1999 See the abstract	10-14

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 FEBRUARY 2002 (15.02.2002)	18 FEBRUARY 2002 (18.02.2002)

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 920 Dunsan-dong, Seo-gu, Daejeon Metropolitan City 302-701, Republic of Korea Facsimile No. 82-42-472-7140	JEON, Il Yong Telephone No. 82-42-481-5981